UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/764,790	01/17/2001	Mark L. Antes	5577-221	7193

20792 7590 05/14/2004

MYERS BIGEL SIBLEY & SAJOVEC
PO BOX 37428
RALEIGH, NC 27627

EXAMINER	
SALL, EL HADJI MALICK	
ART UNIT	PAPER NUMBER
2157	

DATE MAILED: 05/14/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

## *Office Action Summary*	**Application No.** 09/764,790	**Applicant(s)** ANTES ET AL.	
	Examiner El Hadji M Sall	**Art Unit** 2157	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE ____ MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 January 2001*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-23* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 5.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

This action is responsive to the application filed on January 17, 2001. Claims 1-23 are pending. Claims 1-23 represent methods, systems and computer program products for providing failure recovery of network secure communications in a cluster computer environment.

Double Patenting

1. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and, *In re Thorington,* 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

2. Claims 1-23 are provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-23, of copending Application No. 09/764,500. Although the conflicting claims are not identical, they are not patentably distinct from each other because they recite means or steps that are substantially the same and that would have been obvious to one of ordinary skill in the art. 37 CFR 1.78(b) provides that when two or more applications filed by the same applicant contain conflicting claims, elimination of such claims from all but one application may be required in the absence of good and sufficient reason for their retention during pendency in more than one application. Applicant is required to either cancel the conflicting claims from all but one application or maintain a clear line of demarcation between the applications. See MPEP § 822.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-8, 20 and 22 are rejected under 35 U.S.C. 102(b) as being anticipated by Francis et al. (US 05/652,908)

Francis teaches the invention as claimed including methods, systems and computer program products for providing recovery of network secure communications in a cluster environment (see abstract).

As to claim 1, Francis teaches a method of recovering from a failure of a primary distribution processor which provides secure communications over a network in a distributed workload environment having target hosts which are accessed through the primary distribution processor by a common network address (figure 1), the method comprising the steps of:

providing to a backup distribution processor information sufficient to restart communications through the primary distribution processor utilizing network security (column 4, lines 21-24, Francis discloses the control server provides centralized control to ensure that console access exists for each resource to be controlled and that the client workstations know how to access each resource and how to recover from component failure);

detecting the failure of the primary distribution processor (column 2, lines 55-58, Francis discloses failure recovery means are provided for detecting and correcting control system failure);

restarting the communications utilizing network security at the backup distribution processor utilizing the provided information (column 2, lines 55-58, Francis discloses failure recovery means are provided for detecting and correcting control system failure by re-establishing client-to-resource connections);

routing both inbound and outbound communications with target hosts utilizing the common network address and which are associated with a secure network communication through the backup distribution processor (column 5, lines 52-55, Francis discloses the control server and the hardware resource servers operate using "frontend" tasks for network communication and "backend" tasks for configuration and resource control); and

processing the inbound and outbound secure network communications at the backup distribution processor so as to provide network security processing of the inbound and outbound communications (column 6, lines 4-5, Francis discloses a security key to be combined with the data sent between the front and backends).

As to claim 2, Francis teaches a method according to Claim 1, further comprising the step of maintaining information sufficient to restart communications through the backup distribution processor accessible to at least one distribution processor other than the backup distribution processor (column 4, lines 24-39, Francis discloses Control server 160(figure 1) manages the network based upon configuration data stored in a database 162(figure 1)...this data is maintained to assure that each resource is under the control of a console and for use by fallback processing routines to re-establish communication in the case of a failure)

As to claim 3, Francis teaches a method according to Claim 1, wherein the step of providing information sufficient to restart communications comprises the steps of transmitting network security information from which network security relationships associated with the communications through the primary distribution processor utilizing network security can be re-established at the backup distribution processor from the primary distribution processor to the backup distribution processor prior to failure of the primary distribution processor (column 6, lines 51-55, Francis discloses the administrative program collects the information necessary to update the configuration data to add a resource, or to change resource access paths or fallback paths and transmits it for update over token ring...) .

As to claim 4, Francis teaches a method according to Claim 1, wherein the step of providing information sufficient to restart communications comprises the step of storing in a common storage accessible to the backup distribution processor, network security information from which network security relationships associated with the communications through the primary distribution processor can be re-established at the backup distribution processor (figure 8).

As to claim 5, Francis teaches a method according to Claim 4, wherein the step of restarting the communications utilizing network security at the backup distribution processor utilizing the provided information, comprises the following steps carried out by the backup distribution processor:

obtaining the network security information from the common storage (column 5, lines 50-55, Francis discloses ...the present invention employs interprocess security to enhance the reliability of the server tasks. The control server and hardware resource servers operate using “frontend” tasks for network communication and “backend” tasks for configuration and resource control);

establishing the security relationships associated with the communications through the primary distribution processor at the backup distribution processor (column

2, lines 55-58, Francis discloses failure recovery means are provided for detecting and correcting control system failure by re-establishing client-to-resource connections); and

notifying target hosts associated with the communications that the backup distribution processor has taken ownership of the communications (figure 8).

As to claim 6, Francis teaches a method according to Claim 5, further comprising the step of clearing the network security information from the common storage subsequent to the backup distribution processor obtaining the network security information from the common storage (column 5, lines 20-24, Francis discloses the control server accesses the configuration database 162(figure 5) to determine configuration fallback data (614)...).

As to claim 7, Francis teaches a method according to Claim 5, further comprising the step of storing in the common storage, network security information from which network security relationships associated with the communications through the backup distribution processor can be re-established at another distribution processor (figure 8).

As to claim 8, Francis teaches a method according to Claim 5, further comprising the step of identifying as non-distributed communications, communications to the backup distribution processor utilizing network security which were previously distributed communications routed through the primary distribution processor (column 6, lines 3-8, Francis discloses...this key must be such that interception and modification of an authorized message is detected and that it be difficult to decompose the key to reverse engineer the security algorithm).

Claims 20 and 22 do not teach or define any new limitations above claims 1-8 and therefore are rejected for similar reasons.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 9-19, 21 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Francis as applied to claim 1-8 above, and further in view of Martin et al (IBM SG24-5309-00).

Francis teaches the invention substantially as claimed including providing failure recovery of network secure communications in a cluster environment (see abstract)

As to claim 9, Francis teaches the method of claim 5 above.

Francis fails to teache the limitation further including the network security comprises Internet Protocol Security (IPSec) (See column 5-6).

However, Martin teaches the network security comprising Internet Protocol Security (IPSec) (page 37, lines 21-22, Martin discloses the IP Security Architecture (IPSec) provides a framework for security at the IP layer for both IPv4 and Ipv6)

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Francis in view of Martin so that the network security comprises Internet Protocol Security (IPSec). One would be motivated to do so to provide better security in the common storage, and between the clients, the servers or distributing processors.

As to claim 10, Francis teaches the method of claim 9.

Francis fails to teach the limitation further including IPSec, and the network security information stored in the common storage includes at least one of Phase 1 Security Association (SA) information, Phase 2 SA information and information relating the Phase 1 SA information to the Phase 2 SA information.

However, Martin teaches the network security information stored in the common storage includes at least one of Phase 1 Security Association (SA) information (page 47, section 3.2.3, Martin discloses during Phase 1, the partners exchange proposals for the ISAKMP SA and agree on one...), Phase 2 SA information and information relating the Phase 1 SA information to the Phase 2 SA information (page 47, section 3.2.4, Martin discloses during phase 2, the partners exchange proposals for protocol SAs and agree on one)

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Francis in view of Martin so that the network security information stored in the common storage includes at least one of Phase 1SA information, Phase 2 SA information and information relating the Phase 1 SA information to the Phase SA information. One would have been motivated to do so to establish security associations that are needed by the common storage

As to claim 11, Francis teaches a method of recovering from a failure of a first routing communication protocol stack which routes between a network and a plurality of application instances executing on a cluster of data processing to a plurality of target communication protocol stacks detecting failure of the first routing communication protocol stack at a second routing communication protocol stack (column 4, lines 21-24, Francis discloses the control server provides centralized control to ensure that console access exists for each resource to be controlled and that the client workstations know how to access each resource and how to recover from component failure);

reading information from coupling facility of the cluster of data processing systems(column 6, lines 5-8, Francis discloses this key must be such that interception and modification of an authorized message is detected...).

Francis fails to teach the limitation further including the steps of: reading IPSec information associated with the at least one DVIPA from a coupling facility of the cluster of data processing systems; renegotiating IPSec SAs between the second routing communication protocol stack and remote IPSec peers utilizing the at least one DVIPA based on the IPSec information read from the coupling facility; re-routing the connections to the at least one DVIPA utilizing IPSec through the second routing communication protocol stack; and performing IPSec processing for the re-routed connections to the at least one DVIPA at the second routing communication protocol stack utilizing the renegotiated IPSec SAs (figure 10).

However, Martin teaches the steps of: reading IPSec information associated with the at least one DVIPA from a coupling facility of the cluster of data processing systems; renegotiating IPSec SAs between the second routing communication protocol stack and remote IPSec peers utilizing the at least one DVIPA based on the IPSec information read from the coupling facility; re-routing the connections to the at least one DVIPA utilizing IPSec through the second routing communication protocol stack; and performing IPSec processing for the re-routed connections to the at least one DVIPA at the second routing communication protocol stack utilizing the renegotiated IPSec SAs (page 37-44).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Francis in view of Martin so that the above steps are achieved. One would be motivated to do so to provide better security in a process failure recovery. It would provide integrity in the data transmitted or stored, and detect any unauthorized message.

As to claim 12, Francis teaches the method of claim 11 above.

Francis fails to teach the step of renegotiating IPSec SAs comprises the steps of: notifying an instance of an Internet Key Exchange (IKE) application associated with the second routing communication protocol stack of the failure of the first routing communication protocol stack;

providing the read IPSec information to the IKE application;

negotiating new IPSec SAs associated with the at least one DVIPA utilizing the IKE application; and

installing the new IPSec SAs in the second routing communication protocol stack (columns 5-6, lines 50-67 to lines 1-44).

However, Martin teaches the step of renegotiating IPSec SAs comprises the steps of:

notifying an instance of an Internet Key Exchange (IKE) application associated with the second routing communication protocol stack of the failure of the first routing communication protocol stack; providing the read IPSec information to the IKE application;

negotiating new IPSec SAs associated with the at least one DVIPA utilizing the IKE application; and

installing the new IPSec SAs in the second routing communication protocol stack (pages 45 – 47)

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Francis in view of Martin so that using IKE, the above steps can be achieved. One would have been motivated to do so to establish security associations, keys need to be formed in a secure and protected manner and IKE provides the mechanism to achieve this.

Claims 13-19, 21 and 23 do not teach or define any new limitations above claims 9-12 and therefore are rejected for similar reasons.

Conclusion

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to El Hadji M Sall whose telephone number is 703-306-4153. The examiner can normally be reached on 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ario Etienne can be reached on 703 308-7562. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

E Hadji Sall
Patent Examiner
Art Unit: 2157

SALEH NAJJAR
PRIMARY EXAMINER